

White Paper

Optivity Policy Enabled Networking

A policy-based approach to Application Optimized Networking

NORTEL
NETWORKS™

How the world shares ideas.

Optivity Policy Enabled Networking

A policy-based approach to Application Optimized Networking

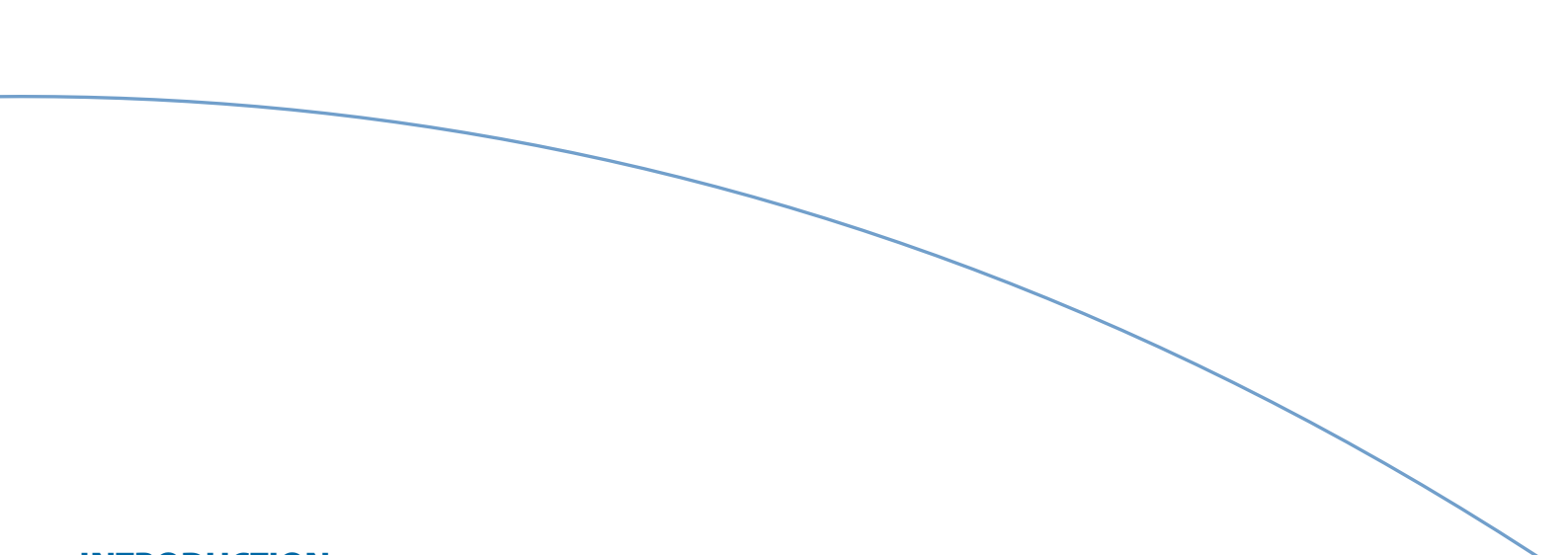
ABSTRACT

To successfully deploy applications, organizations need an intelligent network infrastructure, and network systems management. Thus armed, organizations can bind business policies to the allocation of network resources. Network administrators must provision network resources through policies if they are to achieve an application-optimized network.

Policy management is an emerging solution set that enables business-critical applications to perform at specific levels for specific users. It implements a set of rules or policies that further an organization's business objectives by dictating how users, applications, and organizations can access and use network resources.

Nortel Networks' Optivity Policy Enabled Networking strategy enables both enterprises and service providers to meet policy management's demands. It does so by offering voice and data solutions that are reliable, differentiated, scalable, and secure. This paper focuses on enterprise solutions but does make reference to evolving service provider solutions.

Policy management is one of the key aspects of Nortel Networks' Unified Networks strategy.



INTRODUCTION

The Internet and emerging Web technologies are having a profound effect on how business is conducted now and in the future. The importance of the telecommunications network to the enterprise bottom line continues to increase as steady streams of business-critical applications are introduced.

As a result, enterprise networks (and its managers) are being tested and pushed to the limit. Without the right tools, few enterprise networks will be able to offer the application predictability that the business demands, nor will they be able to effectively introduce new applications to exploit new business opportunities and support existing ones.

The challenges facing the enterprise manager include:

- **Network Congestion** — Bandwidth-intensive applications adding load to the network. Networks are struggling with the realities of providing acceptable Quality of Service (QoS) to mission-critical applications, while also meeting the needs of the day-to-day user. The cost of adding bandwidth in the WAN to increase application performance is prohibitive and still provides no guarantees that mission-critical applications receive priority service.
- **Application Predictability** — As new applications emerge, they compete for network resources with existing applications. The enterprise network must be able to specify the relative resource priority of these applications.

- **Administrative Challenges** — As organizations implement new applications, the number of administration systems in the network also increases. As a result, network managers are faced with the increasingly difficult task of administering the network to manage the needs of users and the differing priority requirements of the applications.
- **Network Complexity** — The typical enterprise network is heterogeneous; oftentimes, the full potential of each element is not taken advantage of. Even under a best-case scenario, the network must be managed on a device by device basis.
- **Security** — The network manager is faced with the difficult task of meeting internal and external security requirements while still providing easy and timely access to network resources to authorized users.

The solution to these issues lies in policy management and policy enabled networks — enabling networks to bring predictability and control to business-critical applications. This solution must enable business-critical applications to receive preferential treatment from the network and minimize the complexity of end-to-end management and security.

In policy enabled networks, the network is automatically aware of who is trying to do what. It correlates information about each user and the application running, taking into account the three major aspects of users on the network:

- Security Characteristics
- Business Priorities
- Network Characteristics

These are used to determine if the user is authorized to run a particular application and, if so, what priority the user should receive and the amount of the network resources, (e.g., bandwidth), should be allocated. For example, the user surfing the Internet may be given a lower priority than the person running a mission-critical application.

As it evolves, policy management will provide the enterprise with a simple, unified solution to better meet current and future needs.

POLICY MANAGEMENT OVERVIEW

Policy Management enables the enforcement of a set of rules or policies that dictate access rights and use of resources based on the established profile of the application, user, and group, to meet an established business objective. A comprehensive policy management solution will provide three elements – provisioning, enforcement, and verification of the policies.

Policy management is essentially focused on providing QoS (bandwidth, latency, priority) and security (authentication, authorization, auditing) end-to-end across the network, and consists of the building blocks shown in Figure 1.

POLICY MANAGEMENT COMPONENTS

Advanced Directory

Historically, directories have been application-specific. However, from file and Internet directories, to e-mail and remote access directories, network managers are overwhelmed by the requirements of maintaining multiple separate directories. As employees or resources are moved, added, or deleted, the effort in modifying all the directories involved is considerable. Furthermore, network managers are also faced with the daunting task of integrating and managing the additional directories that invariably come with new applications, with those already present in the network.

Since much of the information contained in any one directory is often duplicated in a number of others, the goal should be the consolidation and linking of these disparate directories into what is, in effect, a single global directory — an advanced directory.

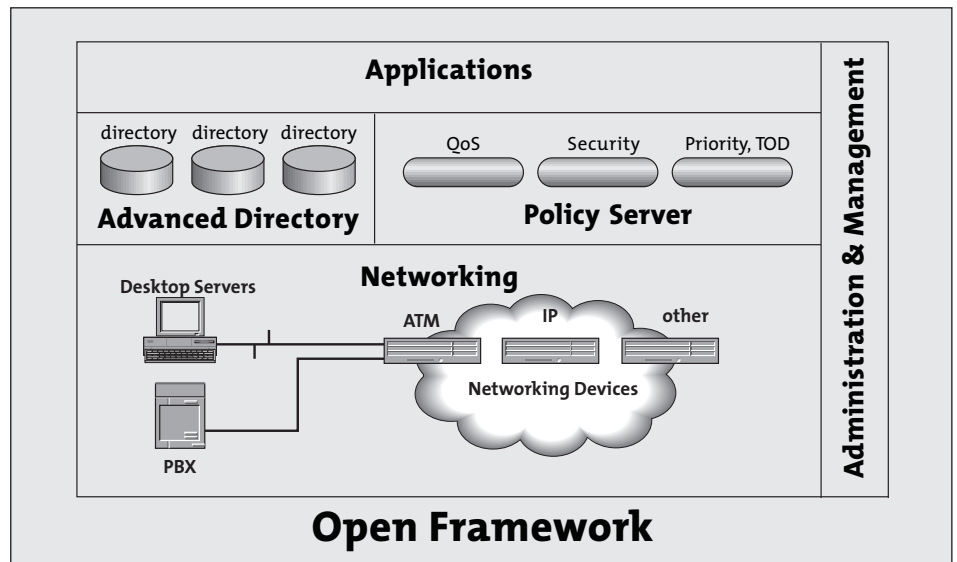


Figure 1 - Policy Management Building Blocks

An advanced directory achieves this by adhering to a common schema and interfacing with a policy server that enforces set rules or policies. The implementation of an advanced directory results in the strengthening of the network where repetition of information and directory overlap is reduced.

In such a scenario, the directory becomes a key component of the network. Policies, user information, network configuration data, and network addresses are all found in one "central" location. The benefits of creating this "virtual" central directory (virtual in the sense that the directories are linked together to appear as one) are tremendous. The savings in administration and management labor costs alone can be quite significant.

However, to achieve the benefits of policy management, a logically centralized directory must have the ability to be distributed, replicated, partitioned, and extended. Without such features, the goal of simplifying current network management infrastructures will fail.

Distributed: The performance impact of maintaining a large organization's directory service on one server is prohibitive. A distributed directory service enables the information to be spread over several servers (geographically, or by management domain), maximizing network performance and manageability, and improving local control.

Replicated: The spread of information from one server to the next is essential as the network grows or information changes. Without replication, network maintenance and management remains a cumbersome process since each separate management domain must be configured individually.

Partitioned: Partitioning allows for sensitive or critical information to be located in more secure areas of the directory, making it less vulnerable to unauthorized access. Furthermore, by partitioning sections of the directory into other domains within the network, managing user information is made easier as policies can be set based on an assessment of the local network state.

Extensible: With policy management still in its infancy, a directory service must be able to grow and expand as new standards or applications evolve. Unless the directory is capable of evolving over time, the effort and costs of implementing and constantly upgrading such a system will be prohibitive.

Having recognized the significant potential benefits of unified directory services, a number of vendors have recently introduced directory products designed to meet the demands of policy-based networking. Some of the competing solutions include Netscape's Directory Server, Novell's Directory Service (NDS), Microsoft's Active Directory, ICL's i500 Directory, Sun Microsystems Inc.'s Sun Directory Services, and Banyan Systems Inc.'s Streettalk — just to name a few.

Policy Server:

Policy servers will be a key component of any policy management system. The policy server is responsible for gathering all of the relevant information, making a decision based on the administrator's set policies and network resources, and then communicating that decision to the access node via a policy transaction protocol such as Common Open Policy Service (COPS). The goal of the policy is to ensure that a request from a specific application, user, or group is valid and that the application, user, or group receives the proper service (bandwidth, ACLs, QoS). These decisions will be based on business priorities, security requirements, and network capabilities involving QoS, user access, and authentication. This approach reduces network administration while increasing management control over valuable network resources.

To carry out the policy set by the administrator, the policy server generally:

1. Receives service requests or queries from network devices/applications/....
2. Retrieves policy from the advanced directory.
3. Retrieves other data such as network availability or utilization, time-of-day, or Service Level Agreement (SLA) information to develop an action consistent with the policy. This information can use static directory information and/or real-time network information.
4. Communicates the policy decision to the policy enforcement device (e.g. switch/router) using a policy transaction protocol such as COPS Simple Network Management Protocol (SNMP), or command-line interface (CLI).
5. In some cases, the policy server may be required to notify the end devices. In this case, a notification is sent to the enforcement device that initiates a request for the policy change from the policy server.
6. Through a feedback mechanism, receives dynamic information from the network to validate or adjust current policy to ensure users receive required level of service.

Administration and Management

A solid policy enabled networking strategy must be closely tied to Internet Protocol (IP) address management and network management. While an administrator sets policies at the user level, edge devices only recognize IP addresses. An IP address management tool binds a user to an IP address and, through support of Dynamic Host Configuration Protocol (DHCP), keeps this address dynamically updated. With this functionality, administrators are

able to define policies according to users or applications that they recognize, and the information will be abstracted to an IP address that the edge device recognizes. Network management provides the topology awareness required to bind session traffic to the appropriate physical network path. Network management also provides the feedback loop required through Service Level Management (SLM) to ensure that policies are being enforced.

With a policy management infrastructure, administration and management of the network can be less complicated. Using a common directory schema, the network manager can outline a configuration schema for a specific device type. Devices no longer need to be configured individually, greatly reducing the time and effort currently required. This can be extended to simplify device configuration in multi-vendor networking environments.

Ongoing management of the network is also made easier through the ability of a policy management system to replicate, store, and synchronize policy information across the directory service.

Applications

From network management applications to business critical applications, these are the functions that need to leverage the information and access parameters in the policy management framework. These enterprise applications are demanding higher levels of predictability and availability (in terms of QoS and security). Depending on your point of view, applications need to become more network-aware, or perhaps the network needs to become more application-aware. In either case, there needs to be a stronger link between the two — such is the goal of policy management.

Networking

Networking provides the transport of traffic and enforcement of the policy for that traffic. Each device along the traffic's path will have its local policy mechanism, which will be coordinated by the policy server to deliver the end-to-end policy. Because each device along the path may not be owned or managed by a single organization, there needs to be a signaling mechanism to enable the establishment of an end-to-end policy.

Policy Attributes

A comprehensive policy management solution will be responsible for the provisioning, enforcement, and verification of the following policy attributes:

Quality of Service (QoS): This is a determination of how to allocate resources, primarily through DiffServ and IntServ, such as bandwidth and network latency.

Priority and Time-of-Day (TOD): This is determining the relative or absolute allocation of resources to a user under normal or abnormal network conditions. For example, a policy may dictate that a customer accessing an online help system takes priority over internal employee access to a Dilbert web page.

Security: As enterprise networks open up for external access and more business-critical resources are available on the network, security has become more critical in controlling who has what level of access to what resources. Some key issues are as follows:

- **Internet:** The Internet offers low cost, ubiquitous access, but it was never designed to be secure. As well, hackers from other countries with different laws can inflict damage or steal information without repercussion

- **Remote Access:** Allows use of the public network for small office/home office (SOHO) and road warriors, but adds to the complexity of determining the level of access
- **Internal Communications:** Studies have shown that approximately 80% of network violations are from internal users. Security within the campus and restricted outbound access are becoming issues.
- **Business Critical Applications:** Applications such as e-commerce demand a high level of privacy, and are required by enterprises to remain competitive
- **Complexity:** Security is often seen as a necessary evil – it usually decreases throughput and is complicated. The level of security is only as good as how well it is implemented and maintained. The enterprise manager must weigh the level of security warranted against the cost and complexity of maintaining the system.
- **Performance:** Analyzing each packet introduces extra hardware to handle the processing.

Whereas firewalls have been the primary security mechanism in most enterprises, it is now recognized that they do not provide all the functionality and capabilities required. Firewalls are very efficient at controlling who does and does not get access, but they are not equipped to control levels of access and privacy.

IP networks are inherently vulnerable to security risks such as spoofing and session eavesdropping. This is unacceptable for developing business requirements, such as e-commerce. Both users and the business need to feel confident that personal infor-

mation is secure. Without security, these initiatives are almost certainly doomed to failure.

To address these issues, a standard solution has been developed. IP Security (IPSec) is a collection of protocols from the IETF designed to ensure that data crossing an IP network is both protected and secure. IPSec adds authentication and encryption to all IP communications. Its authentication features let network managers guard against attacks launched either internally or externally. IPSec also allows network managers to choose just what kind of encryption they want to use.

However, secure data alone is not enough. New applications such as e-commerce demand capabilities such as non-repudiation of transactions and secure messaging.

The foundation of e-commerce requires the use of digital certificates that enable public key cryptography. Public Key Infrastructure (PKI) is a collection of services required to issue and manage these digital certificates. Entrust Technologies' product portfolio provides the most comprehensive set of PKI life-cycle services available for the enterprise today, leading the way in solutions enabling the deployment of widespread e-commerce.

With these systems in place, there is still the requirement to audit the network to ensure that the security policies are enforced and meet the business requirements of the enterprise. Whether through malicious attacks or incomplete security policies, intrusion detection systems play a vital role in assuring that as access is given, actions are not taken which are contrary to business objectives. This audit analysis can then be used to fine-tune the security policies.

In conjunction with the X.500 Global Directory Service, and evolving standards such as Directory Enabled Networks (DEN) and Lightweight Directory Access Protocol (LDAP), these systems and technologies promise to help establish a single, and secure, directory structure with a viable directory interface.

NORTEL NETWORKS POLICY MANAGEMENT STRATEGY

Nortel Networks provides the unique capability set provided by Bay Networks, a Nortel Networks Business, and Nortel. Bay Networks has a strong history of IP networking and enterprise management through the Optivity network management product line. Nortel has a proven history of providing robust QoS-enabled networks and global deployment experience. Through the implementation of its own internal corporate IP network — one of the largest in the world — Nortel Networks has come to understand what it takes to support a secure and dynamic network, providing a much clearer view of a customer's needs.

The scope of policy management can be very large and unwieldy if the focus is not on offering customer value. The objective of Nortel Networks strategy is to take full advantage of existing network capabilities while providing a smooth transition toward the network of the future. The goal is to deliver an integrated policy management framework to allocate resources in multi-vendor networks that support customer business goals and provide increasingly capable QoS and security features across the Nortel Networks data networking product line.

Nortel Networks policy management solution consists of an end to end solution for provisioning, enforcement, and verifica-

tion. It provides a framework that allows network managers to define policies for prioritization and access on the network, enforce the policies during network operation by interacting with application/user request for priority or access, and verifying that policies are being met through ongoing monitoring of application service level performance.

Nortel Networks framework encompasses the following customer values:

- Business priorities: Give customers the ability to map their application behavior to business priorities.
- IP plus: Although IP is prevalent as an access and networking protocol, other services, such as voice over IP (VoIP), also need to be integrated into the policy management framework.
- Reduce complexity: Nortel Networks vision of policy management is to assist in the simplification of running network services, as well as to enable the enterprise to take full advantage of network services.

- Standards-based open framework for extensibility and heterogeneous networks – multi-directory/multi-vendor
- Consistent framework across enterprise network services: Whether deploying remote access or intranet services, the framework must be consistent. All capabilities used in each case may not be the same, but the general process must be the same
- Fit into service providers: Service providers are often used for the transport of enterprise traffic between sites. It is the responsibility of the service provider to provide transport capabilities that meet the requirements of the enterprise policy according to established SLAs. To ensure that an end-to-end policy is in place, a process involving the mapping of policy between enterprise and service provider networks will need to take place.

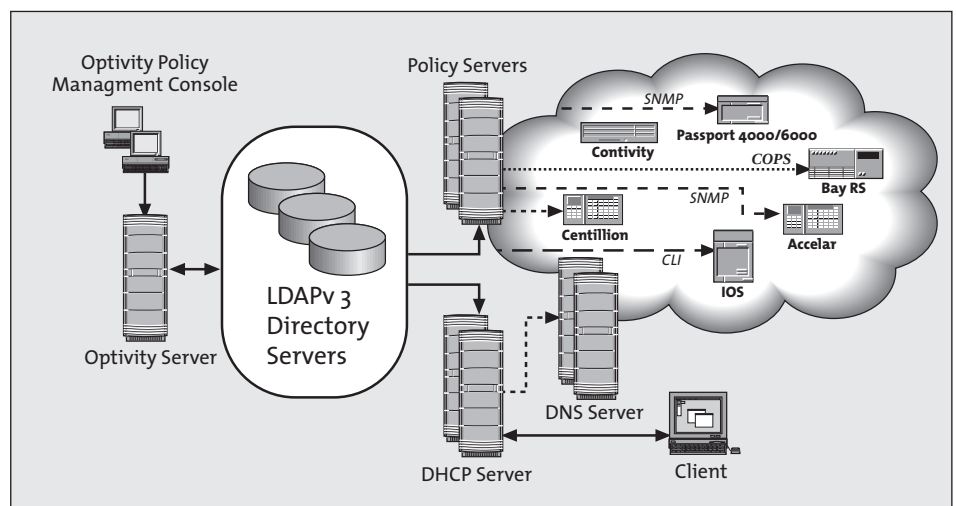


Figure 2 – Nortel Networks Policy Management Strategy

The solution leverages Nortel Networks strengths in IP services and network management to deliver an effective policy management framework and simplify the deployment of policy-based networking. The Optivity policy management console is an extension of Bay Networks NetID IP address management solution, with additional capabilities for creating user profiles and specifying application priority levels. These policies are stored in a standards-based policy directory where they will then be translated into the specific device configuration settings that will, in turn, change the behavior of the network device according to the policy. This mapping of policies into device configuration settings will heavily leverage the Optivity Network Configuration System (NCS); the industry's only system-oriented, multi-vendor, network configuration management solution. Optivity NCS first creates the device configuration settings and the distributes them to the devices throughout the network. Optivity Service Level Management provides a key component to policy management by providing a system for continuously verifying that policies are being met. By monitoring application service level performance, Optivity Service Level Management closes the loop by reporting the network's ability to deliver application service levels that are compliant with business objectives.

Nortel Networks framework is designed to support a DEN-compliant schema within any LDAPv3-compliant directories. This provides flexibility for enterprises to select the directory which best fits their needs while avoiding the proliferation of multiple directories. The explicit association with users is the tie-in with directory services. Development in this area includes relationships with such leading networking software vendors as Microsoft, Novell, and Netscape. No other vendor can make this claim.

NORTEL NETWORKS POLICY MANAGEMENT PRODUCT SOLUTIONS

An application-optimized network comprises several new elements that do not exist in networks today. Nortel Networks will deliver these elements in three phases over the next two years. Each phase brings more application predictability and network control. The diagram illustrates the phased rollout of the Nortel Networks policy management solution.

Optivity Policy Services 1.0

The first release or phase of Optivity Policy Services begins to map the existing infrastructure and application priorities to business objectives by leveraging DiffServ and priority queuing mechanisms. Through a policy management interface, policy definition, management and configuration can be centrally managed, allowing for the static definitions of application policies across the enterprise infrastructure. This will enable more predictable application behavior with lower response

times and higher availability for applications against which policies are defined. The policy server will automatically reconfigure devices, eliminating the need to manually configure QoS on individual devices. The devices will be configured to respond in accordance with the policies whenever they are handling traffic that can be identified as belonging to those applications.

Policies will be stored within a DEN-compliant schema in an LDAPv3-compliant directory and will be translated to a source IP address that the edge device recognizes through IP address management and directory services integration.

With this initial implementation, a network administrator will define a policy from the policy management console by setting a specific level of service. For instance, assume a system administrator has defined SAP as a premier application that requires preferential treatment over others. The policy consists of attributes and actions. In this case, the action would be that SAP traffic is set at TCP Port 1492.

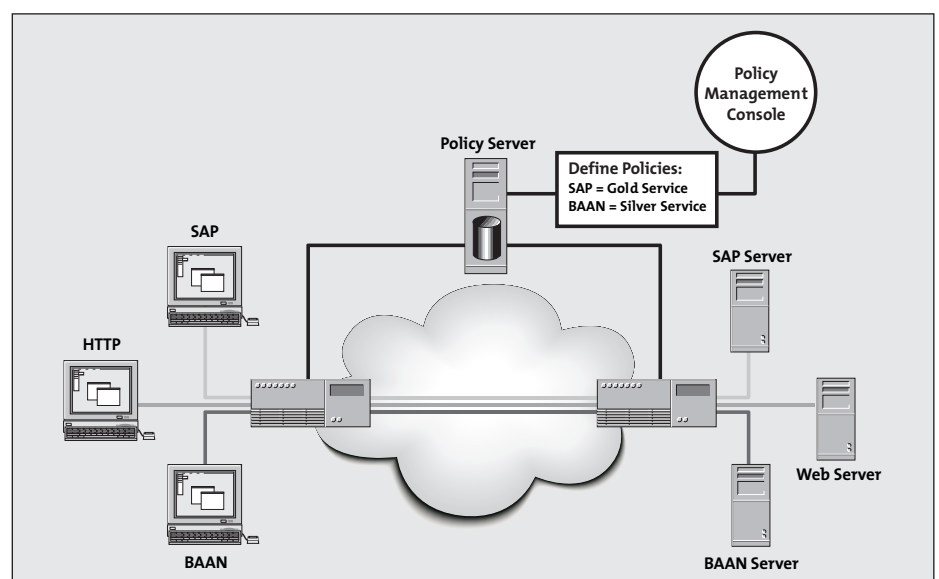


Figure 3 - Nortel Networks' Policy Management Solutions

As a result of this policy, the Policy Server sets a filter on the network device. The Policy Server communicates with the network device via the COPS or Command Line Interface (CLI). Once the Policy Server has updated the network infrastructure – whenever a device that is in-between a SAP client and its servers detect a flow of SAP traffic – it prioritizes that traffic over other traffic. This of course relies on the network devices having the ability to identify traffic as SAP, and the ability to treat it differently as it passes through the device. If a policy has not been defined, best effort service continues to apply.

This first release of Optivity Policy Services leverages the application intelligence already found in customers' existing network infrastructure.

Accelar Routing Switches: IP routing, deep packet filtering and priority queuing

Bay Networks Routing Services

(BayRS) – Resource Reservation Protocol (RSVP), (DiffServ and Intserv), Progressive Traffic Management

Passport Enterprise Networking and Multiservice Switches

– IP QoS over ATM, IP routing, packet filtering, sophisticated ATM/frame relay wide area network (WAN) traffic shaping and policy

Cisco IOS – DS byte manipulation, priority queuing

One essential ingredient in getting any real value from policies is being able to measure the effect of these policies in terms of application performance. With Service Level Management capabilities already built into Optivity, application

behavior can be measured, compared, and correlated with network events and the policies in force. This provides network managers with the information that they need to refine policies for better results or upgrade the infrastructure where that is more appropriate.

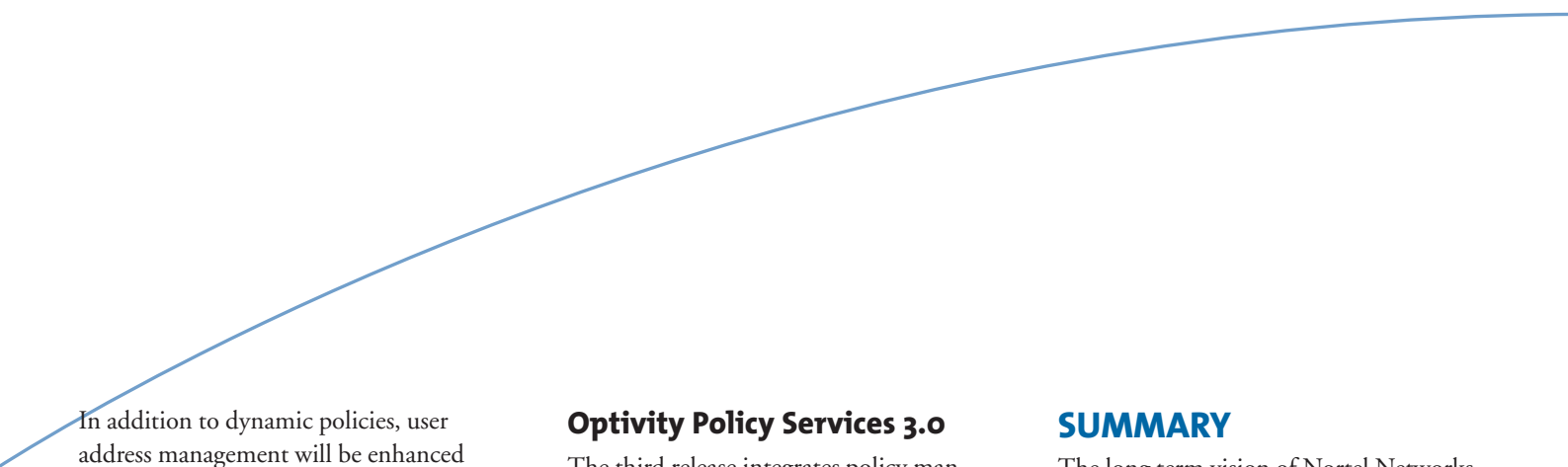
As discussed earlier, tight integration between IP address management and network management is also required. While a system administrator defines policies based on a user, the network devices that enforce the policies recognize an IP address. Bay Networks NetID IP address management solution provides the capability to abstract the user to an IP address. DHCP support provides the dynamic association between user and IP address that policy-enabled networking requires.

Optivity Policy Services 2.0

The second release of Optivity Policy Services moves to an increasingly dynamic model in which the network can respond more intelligently to potential contention for availability of resources. This will include Resource Reservation Protocol (RSVP) admission control. In the first release of Optivity Policy Services, applications can be prioritized but there is no control over how much bandwidth they can consume, potentially leaving the network open to over-subscription. Consequently, even with static policies in force, this could result in variable application response, although it would be better than in an uncontrolled network.

With Optivity Policy Services, dynamic policy enforcement introduces more sensitivity to available resources and provides a mechanism for dynamic allocation of the resources based on policies. For example, a policy might stipulate that video applications cannot consume more than 50 per cent of available bandwidth. Suppose that SAP is already running and receiving priority service, and another user starts a videoconference. The first application-intelligent device that detects the video session would query the policy server for a ruling on how to treat the traffic.

Suppress it, slow it down, or prioritize it – the action will depend on how the network is currently being used. Once again, the need for application intelligence is clearly demonstrated. In addition, the network devices will require a mechanism for quickly querying the policy server, and reconfiguring themselves on the fly. Thus, support for new networking protocols (i.e. COPS) will be required for dynamic enforcement



In addition to dynamic policies, user address management will be enhanced through an authenticated user IP address binding. This introduces an additional level of granularity to policy definition and enforcement by allowing for the identification of policies based on users as well as applications. After users have been assigned an IP address, they will be authenticated against their NT or NDS login. For example, say a policy has been created that assigns a user a gold level of service. When the user comes online, he or she receives an address through DHCP and logs in. Policy login software on the NDS or NT server detects that the user has logged in at a specific IP address, such as 141.251.10.3. The software notifies the system that the user is at that specific IP address. The policy server then notifies all devices on the subnet associated with that address to place traffic from IP 141.251.10.3 in the high priority queue.

Optivity Policy Services 3.0

The third release integrates policy management with Optivity's topology database. This makes it possible to dynamically allocate network resources based on current usage, topology and existing policy information. With this information, the policy server can take account of the state of the network at the moment it applies the policies. For example, by examining the end-to-end path between client and server, the policy server could determine whether any of the links are congested and then adjust the performance of other applications so that there is more bandwidth available for a new high priority user or application. This integration also makes it possible to dynamically enter device information from NMS into the policy system.

This release will also offer enhanced accounting and billing features based on the DS byte. This will allow service providers to offer premium services to clients and keep a record of the service provided leveraging the DiffServ technology.

SUMMARY

The long term vision of Nortel Networks is to deliver Unified Networks – a unified IP network infrastructure that spans intranets, extranets, and the Internet and can carry voice, video, and data as required by business applications. Policy Management is a prerequisite for this to occur. If application predictability cannot be delivered for existing data applications, there is little chance of doing so for future applications such as Internet-enabled call centers that will combine voice or video with data.

Nortel Networks strategy for policy management is to deliver an integrated policy management framework that allocates resources across multi-vendor networks. This can be achieved through the integration of policies and service level management with the existing network management and IP management capabilities of Optivity and NetID, and by incorporating and expanding the breadth of application intelligence features (such as QoS) and security across the Nortel Networks data networking product line.

APPENDIX A: ENABLING TECHNOLOGIES

Directory Enabled Networks (D.E.N.):

In the context of policy management, the purpose of a directory service is to store and manage a network's policies. As such, the directory might contain network status information, usage trends, and resource usage. Directories also enable the association of a user's profile to the level of service, access, and priority they will receive. It could also be used to block the browsing of certain web sites. Together, this information can be used to optimize network resource allocation.

The Directory Enabled Network initiative (DEN) is an industry-wide initiative involving more than 20 companies integrating directory services and networks, enabling the development of rich network applications that will operate with a variety of network and directory vendor offerings. The specification defines the directory schema for integrating networks with directory services. Specifically, it defines network elements and services and how they interact with applications, users, and other services. Currently, the Desktop Management Task Force (DTMF) is reviewing the schema. Once the schema is in place, directory/network interaction will become standardized and will simplify integrated multi-vendor policy solutions.

Directory-Enabled Networks is a specification that is designed to integrate directory services with physical networks. DEN can map policy-based intelligent networking services to individualized QoS for specific users or applications. It lets a network owner specify, within the directory, characteristics of how the network should operate - for individual users, classes of users, or applications.

DEN defines a way to retrieve and store information about network policies in a database. Through LDAP, DEN-enabled policy servers will then gather information from the "virtual" directory and match it with specific policies about how bandwidth is allocated across devices, users, and applications.

DEN becomes increasingly important as mission-critical business applications are built on general-purpose intranets, extranets, and the Internet. As these applications compete with lower priority applications such as casual Web browsing, DEN will allow prioritization of bandwidth for specific applications or users. This could, for example, allow payroll data or an urgent customer order to be prioritized (in terms of bandwidth availability) over an employee accessing a Web site. As networks include a mixture of mission-critical and casual applications, it will be critical to judiciously allocate managed network resources appropriately.

X.500 Global Directory Service

X.500 is a series of standards-based protocols that specify a model for connecting local directory services to form one distributed global directory. Local databases hold and maintain portions of the global database and the directory information is made available via local servers. As such, the user perceives the entire directory to be accessible from the local server.

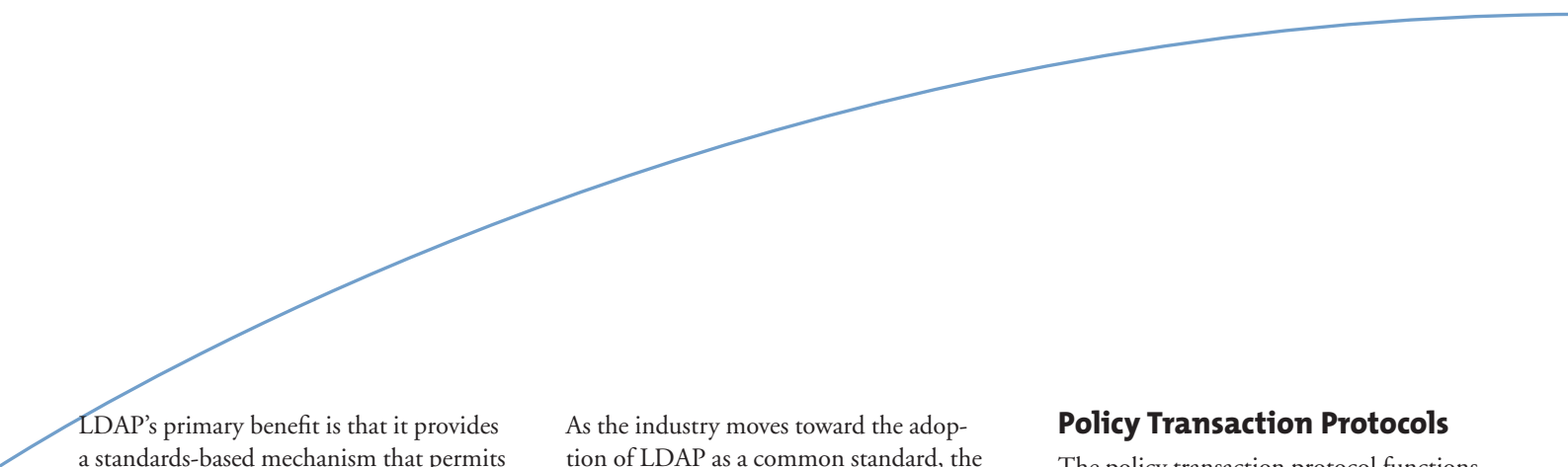
The X.500 directory is organized under a common root directory in a "tree" hierarchy that reflects organizational requirements. Typically, this hierarchy may be based on geographic or organizational boundaries. Each item (entry) in the X.500 directory describes one object (e.g., a person, a network resource, a company)

with a unique identifier called a Distinguished Name (DN). This entry consists of a collection of attributes (e.g. first name, last name, company name, or e-mail address). All entries at each of these levels must have certain attributes in order to adhere to the common schema, or format. However, one of X.500's unique characteristics is that, as long as the common schema is followed, locally established optional attributes are possible, permitting for a flexible, and more manageable solution.

Lightweight Directory Access Protocol (LDAP):

The Lightweight Directory Access Protocol (LDAP) is a revised version of the Directory Access Protocol (DAP). Since it does not require the upper layers of the Open Systems Interconnect (OSI) stack (because it runs directly over TCP/IP), LDAP is a simpler alternative and provides the most important functions of DAP. At the same time, LDAP makes it much easier to implement in servers (especially in clients).

LDAP is a client/server directory access protocol whose purpose is to let different directory services communicate with one another so that users can create and query directories (including Web server and X.500) of people and information, regardless of where or how they're connected. Basically, LDAP's sole purpose is to act as the communications mechanism between the policy server and the directories.



LDAP's primary benefit is that it provides a standards-based mechanism that permits any client, server, or application to access any directory service that supports the LDAP protocol interface. Currently, most products support LDAP Version 2 although LDAP Version 3 is now available. LDAPv3 will add several features including:

- **Security.** LDAPv3 offers an extensible authentication mechanism based on the Simple Authentication and Security Layer (SASL), and encryption and data integrity based on the Secure Sockets Layer (SSL).
- **Simplified schema integration.** LDAPv3 provides clients with the ability to discover the object classes and attributes of their schema
- **Extensibility:** LDAPv3 also allows additional operation to be defined for services not currently available without requiring a change in the protocol version number.
- **Referrals:** LDAPv3 permits an LDAP server to refer a client to another LDAP server if it cannot answer a request for insurance that policies are handled in a timely fashion.
- **International Characteristics.** LDAPv3 has adopted the use of the ISO 10646 character set that permits the use of non-ASCII character sets and non-English conventions to represent data.

As the industry moves toward the adoption of LDAP as a common standard, the ultimate goal is to facilitate the integration of new applications making use of directory services. From personal computers (PCs) to networking components, LDAP will simplify and promote the deployment of directory services across enterprise networks.

Differentiated Services

DiffServ is a method of providing QoS on the Internet. It provides different levels of service by normalizing packet behavior across a network, without the need for per-flow state and signaling at every hop.

This is accomplished by leveraging the TOS octet or DiffServ byte in the IP header. It is used to mark a packet to receive a particular per-hop behavior. A DS byte classifier and per-hop behavior based on these classifications is required in all network devices. For instance, a customer may configure a router with eight queues and use the DS byte to select which queue a packet is placed in for servicing. Devices that do not support DiffServ will leverage queuing to provide differentiated levels of service. For instance, Accelar will initially provide differentiated service through prioritized filters instead of DiffServ. Based on a packet's source and destination IP address, the packet will be moved into a higher or lower queue on the box.

Policy Transaction Protocols

The policy transaction protocol functions as the intermediary between the policy, the policy client, and the policy server. It is responsible for transferring the policy request and policy response between these two nodes. Currently, there are two protocols vying to become the IETF standard for a policy transaction protocol — COPS and DIAMETER. Both protocols are extensible and define a base set of generic operations that can be customized by any service to meet its needs.

COPS is a simple query-and-response protocol for exchanging policy information between a policy server and its client (or clients). Once the policy server makes its policy decision, the policy client is responsible for the enforcement of that particular policy decision. COPS also has the unique feature of allowing the policy control decision to be communicated between the policy client and the policy server in order to determine the validity of that decision. While COPS is currently an RSVP admission control protocol, the IETF is studying the idea of extending it to be a generalized policy communications protocol.

SNMP and RADIUS Because COPS is not yet standard, some of the equipment already deployed will not interoperate with a policy server using these protocols. In these cases, the policy server must translate the policy decision to a protocol that each device can understand. For legacy devices, these protocols will typically be SNMP and RADIUS (the predecessor to DIAMETER).

ACRONYM GLOSSARY

ATM	Asynchronous Transfer Mode	IPSec	IP Security	SSL	Secure Sockets Layer
BayRS	Bay Networks Routing Services	LDAP	Lightweight Directory Access Protocol	SLA	Service Level Agreement
COPS	Common Open Policy Service	NCS	Network Configuration System	SLM	Service Level Management
DTMF	Desktop Management Task Force	NDS	Novell's Directory Service	SASL	Simple Authentication and Security Layer
DAP	Directory Access Protocol	OSI	Open Systems Interconnect	SNMP	Simple Network Management Protocol
DEN	Directory Enabled Networks	PTM	Progressive Traffic Management	TOD	Time-of-Day
DHCP	Dynamic Host Configuration Protocol	PKI	Public Key Infrastructure	TCP	Transmission Control Protocol
DN	Distinguished Name	QoS	Quality of Service	UDP	User Datagram Protocol
IETF	Internet Engineering Task Force	RADIUS	Remote Authentication Dial-In User Services	VoIP	Voice over IP
IP	Internet Protocol	RSVP	Resource Reservation Protocol	WAN	Wide Area Network



How the world shares ideas.

For additional information on Nortel Networks products and services, please contact your Nortel Networks account representative or the office listed below.

United States

Nortel Networks
4401 Great America Parkway
Santa Clara, CA 95054
1-800-822-9638

Canada

Nortel Networks
8200 Dixie Road Suite 100
Brampton, Ontario
Canada L6T 5P6
1-800-466-7835

Europe, Middle East, and Africa

Nortel Networks EMEA, S.A.
Les Cyclades-Immeuble Naxos
25 Allee Pierre Ziller
Valbonne, 06560 France
+33-4-92-96-69-66

Asia Pacific

Nortel Networks Asia South Pacific
151 Lorong Chaun
02-01 New Tech Park
Singapore 556741
+65-287-2877

Caribbean and Latin America

Nortel Networks CALA Inc.
1500 Concord Terrace
Sunrise, FL 33323-2815
954-851-8886

<http://www.nortelnetworks.com>

Copyright © 1999 Northern Telecom, Inc. All rights reserved.

NORTEL, NORTEL NETWORKS, the NORTEL NETWORKS corporate logo and globemark design, HOW THE WORLD SHARES IDEAS Passport, Optivity, Accelar, BayRS, Centillion, Contivity, and NetID are trademarks of Northern Telecom Limited. All other trademarks are properties of their respective holders. Information in this document is subject to change without notice. Nortel Networks assumes no responsibility for errors that may appear in this document.